Divisibility of class numbers: enumerative approach

Yuri F. Bilu and Florian Luca

February 1, 2008

Contents

1 Introduction

It is well-known since Gauss that infinitely many quadratic fields have even class number. In fact, if K is a quadratic field of discriminant D, having r prime divisors, then the class number h_K is divisible by 2^{r-1} if $D<0$ and by 2^{r-2} if $D>0$. See [4, Theorem 3.8.8] for a more precise statement.

In 1922 Nagell [17, Satz VI] obtained the following remarkable result: *given a positive integer ℓ, there exist infinitely many imaginary quadratic fields with class number divisible by ℓ.* See [2] for a different proof.

It took almost half a century to extend Nagell's result to real quadratic field, see Yamamoto [29] and Weinberger [28]. Uchida [27] extended this to cyclic cubic fields. In mid-eighties, Azuhata and Ichimura [3] and Nakano [18, 19] obtained similar results for fields of arbitrary degree n.

Recently Murty [16] gave quantitative versions of the theorems of Nagell and Yamamoto-Weinberger on quadratic fields. He proved that for all sufficiently large X there exist at least $c(\ell)X^{1/2+1/\ell}$ imaginary quadratic fields and at least $c(\ell,\varepsilon)X^{1/4\ell-\varepsilon}$ real quadratic fields with class number divisible by ℓ and discriminant not exceeding X in absolute value. (The second exponent can be replaced by $1/2\ell-\varepsilon$ if ℓ is odd.) Various refinement and extensions of Murty's results were suggested in [5, 15, 25, 30].

Much less is known for fields of higher degree. In [13], it is shown that at least $c(\ell)X^{1/6\ell}/\log X$ pure cubic fields have discriminant not exceeding X and class number divisible by ℓ.

In this paper, we extend these results to fields of degree $n\geq 3$.

Theorem 1.1 *Let n and ℓ be positive integers, $n\geq 3$, and put $\mu=\frac{1}{2(n-1)\ell}$. There exist positive real numbers $X_0=X_0(n,\ell)$ and $c=c(n,\ell)$ with the following property. For any $X>X_0$ there is at least cX^{μ} pairwise non-isomorphic number fields of degree n, discriminant not exceeding X, and the class number divisible by ℓ.*

Actually, we prove slightly more: for all those fields the class group has an element of exact order ℓ.

The famous *Cohen-Lenstra heuristics* [7, 8] predict that number fields of degree $n>1$ with class number divisible by ℓ should have positive density among all number fields of degree n. More precisely, denote by $\mathcal{F}_n(X)$ the set of all non-isomorphic number fields of degree n and discriminant not exceeding X and put $\mathcal{F}_n^{(\ell)}(X)=\{K\in\mathcal{F}_n(X):\ell|h(K)\}$. Then, as $X\to\infty$, the quotient $\left|\mathcal{F}_n^{(\ell)}(X)\right|/|\mathcal{F}_n(X)|$ (conjecturally) tends to a positive rational number, which can be explicitly expressed in terms of certain finite Euler-type products.

This conjecture seems to be out of reach at the present state of our knowledge. Theorem 1.1 implies that number fields of degree n with class group divisible by ℓ have positive *logarithmic* lower density among all number fields of degree n :

$$\liminf_{X\to\infty} \frac{\log\left|\mathcal{F}_n^{(\ell)}(X)\right|}{\log|\mathcal{F}_n(X)|} \geq \frac{2}{(n-1)(n+2)\ell}. \tag{1}$$

This is an immediate consequence of Theorem 1.1 and the inequality

$$|\mathcal{F}_n(X)| \leq c(n)X^{(n+2)/4} \tag{2}$$

due to Schmidt [22] (see also [6, Proposition 9.3.4]). For large n inequality (1) can be refined due to the recent work of Ellenberg and Venkatesh [10].

The argument of the present paper relies on the famous construction of Ankeny-Brauer-Chowla fields [1] and is strongly inspired by the work of Sprindzhuk [26, Section 8.6] and Halter-Koch *et al.* [12]. In Sections 2–4 we collect necessary facts about thin sets and Ankeny-Brauer-Chowla fields. The proof of Theorem 1.1 occupies Sections 5–7.

1.1 Notations and Conventions

All fields in this paper are of characteristic 0. Let K be a field. We write $\bar{K}$ for its algebraic closure. By the Galois group of a separable polynomial $f(x) \in K[x]$ we mean the Galois group of the splitting field of f over K, realized as a subgroup of the symmetric group $\mathcal{S}_n$, where $n = \deg f$. In particular, f is irreducible over K if and only if its Galois group is transitive.

Unless the contrary is stated explicitly (as it is done in Section 3), small letters t, x, y, z with or without indices denote indeterminates algebraically independent over the base field.

Acknowledgements We thank Henri Cohen, Jacques Martinet and Michel Olivier for useful discussions. We are indebted to Władysław Narkiewicz and the referee for drawing our attention to the work of Nagell and Nakano. Yuri Bilu thanks Vera Bergelson for inspiring comments. This work was supported in part by the Joint Project France-Mexico ECOS–ANUIES M02–M01.

2 Thin sets

Let K be a field and let n be a positive integer. Let Υ be a subset of the affine space K^n. The set Υ is called *basic thin set of the first type* if there exists a **non-zero** polynomial $F(\underline{t}) \in K(\underline{t})$ (where $\underline{t} = (t_1, \dots, t_n)$) such that $(\underline{\tau}) \in \Upsilon$ if and only if $F(\underline{\tau}) = 0$. The set Υ is a *basic thin set of the second type* if there exists an K-irreducible polynomial $F(\underline{t}, x) \in K(\underline{t}, x)$ with $\deg_x F \geq 2$ such that $(\underline{\tau}) \in \Upsilon$ if and only if the specialized polynomial $F(\underline{\tau}, x) \in K[x]$ has a root in K. The set Υ is called *thin* if it is contained in a finite union of basic thin sets. It is obvious that the union of finitely many thin sets is thin, and that a subset of a thin set is thin.

Serre [23, Section 9.1] gives a differently looking, but equivalent definition of thin sets.

This following property must be known, but we could not find it in the literature.

Proposition 2.1 *Let L be a finitely generated extension of the field K, and Υ a thin subset of L^n. Then $\Upsilon \cap K^n$ is a thin subset of K^n.*

Proof The case of finite extension L/K is considered in [23, page 128], so we are left with the pure transcendent case. Thus, assume that $L = K(\underline{z})$, where $\underline{z} = (z_1, \dots, z_s)$, and let $\Upsilon \subset L^n$ be a basic thin set of the first type, defined by the polynomial $F(\underline{t}) \in L[\underline{t}]$.

We may assume that K^{n+s} is not a thin subset of itself; otherwise K^n is a thin subset of itself as well (cf. [23, Section 9.4]), and the statement becomes trivial. It follows that F, viewed as a rational function in $\underline{t}, \underline{z}$, is defined and does not vanish at certain $\left(\underline{\tau}', \underline{\zeta}\right) \in K^{n+s}$. Hence, the

polynomial $F_{\underline{\zeta}}(\underline{t}) \in K[\underline{t}]$, obtained from F by specialization $\underline{z} = \underline{\zeta}$, is defined and non-zero. For any $\underline{\tau} \in \Upsilon \cap K^n$ we have $F_{\underline{\zeta}}(\underline{\tau}) = 0$. Hence, $\Upsilon \cap K^n$ is thin.

One argues similarly in the case when $\Upsilon \subset L^n$ is a basic thin set of the second type, defined by the polynomial $F(\underline{t}, x) \in L[\underline{t}, x]$. This time, we find $\underline{\zeta} \in K^s$ such that the polynomial $F_{\underline{\zeta}}(\underline{t}, x) \in K[\underline{t}, x]$ has no factors of x-degree 1. Let $F_{\underline{\zeta}} = G_1 \dots G_k$ be the irreducible decomposition of $F_{\underline{\zeta}}$ in $K[\underline{t}, x]$. Then every G_i is of x-degree at least 2, and $\Upsilon \cap K^n$ lies in the union of the corresponding basic thin sets of the second type. ■

Theorem 2.2 *Let $F(t_1, \dots, t_n, x) \in K[t_1, \dots, t_n, x]$ be a polynomial of x-degree m, and let $s \le n$. Let $G \le \mathcal{S}_m$ be the Galois group of F over the field $K(t_1, \dots, t_n)$. Then for all $(\tau_1, \dots, \tau_s) \in K^s$ outside a thin set the polynomial $F(\tau_1, \dots, \tau_s, t_{s+1}, \dots, t_n, x) \in K[t_{s+1}, \dots, t_n, x]$ is separable, of x-degree m, and its Galois group over $K(t_{s+1}, \dots, t_n)$ is G.*

In particular, if F is irreducible over $K(t_1, \dots, t_n)$, then for all $(\tau_1, \dots, \tau_s) \in K^s$ outside a thin set the polynomial $F(\tau_1, \dots, \tau_s, t_{s+1}, \dots, t_n, x) \in K[t_{s+1}, \dots, t_n, x]$ is irreducible over $K(t_{s+1}, \dots, t_n)$.

Proof The case $s = n$ is treated in [23, Section 9.2, Propositions 1 and 2]. The general case reduces to $s = n$ by Proposition 2.1. ■

Hilbert's irreducibility theorem asserts that K^n is not thin for a finitely generated field K. We shall use the following quantitative version for $K = \mathbb{Q}$, due to S. Cohen [9]. See also Serre [23, Section 13.1, Theorem 1].

Theorem 2.3 *Let Υ be a thin subset of $\mathbb{Q}^n$. Then there exists a positive constant $c = c(\Upsilon)$ such that for $X > 1$ we have*

$$|\Upsilon \cap \mathbb{Z}^n \cap [-X, X]^n| \le cX^{n-1/2} \log X.$$ ■

(For $n = 1$ the log-factor can be omitted.)

3 A special thin set

In this (and only this) section we use capital letters $X, Y, Z, \dots$ for independent variables, reserving small letters $x, y, z \dots$ for algebraic functions.

Proposition 3.1 *Let $K(x)$ be the field of rational functions over K. Let $u, v \in K(x)$ satisfy the following: v has a simple zero (or a simple pole) in $\bar{K}$ which is neither a zero nor a pole of u. Then for any positive integers k and ℓ we have $\big[K(x, u^{1/k}, v^{1/\ell})\colon K(x, u^{1/k})\big] = \ell$.*

Proof Obviously, $\big[K(x, u^{1/k}, v^{1/\ell})\colon K(x, u^{1/k})\big] \le \ell$, so it remains to prove that

$$\Big[K(x, u^{1/k}, v^{1/\ell})\colon K(x, u^{1/k})\Big] \ge \ell.$$

Let $\alpha \in \bar{K}$ be a simple zero (or pole) of v, which is neither a zero nor a pole of u, and let Ord_α be the corresponding place of the field $K(x)$. This place is unramified in the field $K(x, u^{1/k})$, but it is ramified in the field $K(x, u^{1/k}, v^{1/\ell})$, with ramification index ℓ. Hence $\big[K(x, u^{1/k}, v^{1/\ell})\colon K(x, u^{1/k})\big] \ge \ell$, as wanted. ■

Proposition 3.2 *Let K be a field. Consider the polynomial*

$$f(T, X) := (X - a_1) \cdots (X - a_{n-1}) \big(X - \alpha T^\ell - \beta\big) - 1 \in K[X, T],$$

where n, ℓ are positive integers and $a_1, \dots, a_{n-1}, \alpha, \beta \in K^*$. Let $\nu_1, \dots, \nu_{n-1}, \nu$ be integers, $\nu \ne 0$. Let Υ be the subset of K defined as follows: $\tau \in K$ belongs to Υ if for some root ξ of the polynomial $f(\tau, X) \in K[X]$, and for some determination of $\zeta = \big(\xi(\xi - a_1)^{\nu_1/\nu} \cdots (\xi - a_{n-1})^{\nu_{n-1}/\nu}\big)^{1/\ell}$, we have $[K(\xi, \zeta)\colon K(\xi)] < \ell$.

Assume that the polynomial $f(T, X)$ is irreducible over K, and that the polynomial $f(0, X) \in K[X]$ has a simple root in $\bar{K}^*$. Then Υ is thin.

Proof Let $K(x)$ be the field of rational functions and let $t, z \in \overline{K(x)}$ be defined by

$$t = \left(\frac{f(0,x)}{\alpha(x-a_1)\cdots(x-a_{n-1})} \right)^{1/\ell}, \quad z = \left(x(x-a_1)^{\nu_1/\nu} \cdots (x-a_{n-1})^{\nu_{n-1}/\nu} \right)^{1/\ell}.$$

Then $f(t,x) = 0$, and, since f is irreducible, we have

$$[K(x,t)\colon K(t)] = n, \quad [K(x,t)\colon K(x)] = \ell. \tag{3}$$

Also,

$$[K(x,z)\colon K(x)] \geq \ell \tag{4}$$

(consider the ramification at 0).

Further, by the assumption, $f(0,x)$ has a non-zero simple root. This root is distinct from any of the numbers $0, a_1, \ldots, a_{n-1}$. Proposition 3.1 implies that $[K(x,z,t)\colon K(x,z)] = \ell$. Combining this with (3) and (4), we obtain $m := [K(x,z,t)\colon K(t)] \geq n\ell$.

Now let $y \in K(x,z,t)$ be such that $K(x,z,t) = K(t,y)$, and let $g(T,Y) \in K[T,Y]$ be the irreducible polynomial over K such that $g(t,y) = 0$. Then $\deg_y g = m$. Applying Theorem 2.2, we find a thin set $\Upsilon_1 \subset K$ such that for any $\tau \in K \setminus \Upsilon_1$, the polynomial $g(\tau, Y) \in K[Y]$ is of degree m and irreducible over K.

On the other hand, there exists $h(T,X,Z) \in K(T)[X,Z]$ such that $y = h(t,x,z)$. Denote by $d(T)$ the denominator of $h(T,X,Z)$.

Fix $\tau \in \Upsilon$, together with the corresponding ξ and ζ. Then $[K(\xi,\zeta)\colon K] < n\ell \leq m$. Assume that $d(\tau) \neq 0$. Then $h(\tau,\xi,\zeta)$ is a root of $g(\tau,Y)$ of degree $< m$ over K. Hence, either $\deg g(\tau,Y) < m$ or $g(\tau,Y)$ is reducible over K. In both cases $\tau \in \Upsilon_1$.

We have proved that $\Upsilon \subseteq \Upsilon_1 \cup \{\text{the roots of } d(T)\}$. Hence, Υ is thin. ■

4 The Ankeny-Brauer-Chowla fields

Let $a_1, \ldots, a_n$, where $n \geq 3$, be pairwise distinct integers and $f(x) = (x-a_1)\cdots(x-a_n) - 1$. It is well-known that $f(x)$ is an irreducible polynomial [21, Problem 8.121]. The number fields, defined by such polynomials, are called *Ankeny-Brauer-Chowla fields* [1] (ABC-fields in the sequel).

Let ξ be a root of f. The main property of the ABC-fields is that, under mild assumptions about the numbers $a_1, \ldots, a_n$, the field $K = \mathbb{Q}(\xi)$ is totally real, and the numbers $\xi - a_1, \ldots, \xi - a_{n-1}$ form a full rank system of units of K.

Below we summarize the properties of the Ankeny-Brauer-Chowla polynomials and fields, to be used in this paper. In the sequel, $a_1, \ldots, a_{n-1}$ are fixed pairwise distinct integers, a runs in the set of integers distinct from any of $a_1, \ldots, a_{n-1}$, and $f_a(x) = (x-a_1)\cdots(x-a_{n-1})(x-a) - 1$. Unless the contrary is stated explicitly, implicit constants in this section depend only on $a_1, \ldots, a_{n-1}$. In particular, *sufficiently large* means *exceeding a positive constant depending on* $a_1, \ldots, a_{n-1}$.

Proposition 4.1 *Assume that $|a|$ is sufficiently large. Then we have the following.*

1. *The polynomial $f_a(x)$ has n real roots $\xi_1, \ldots, \xi_{n-1}, \xi$ satisfying*

$$|\xi_k - a_k| \ll |a|^{-1} \quad (k = 1, \ldots, n-1), \tag{5}$$

$$|\xi - a| \ll |a|^{1-n}. \tag{6}$$

   In particular, the number field $K_a := \mathbb{Q}(\xi)$ is totally real.

2. *The discriminant of the field K_a is $O\left(|a|^{2(n-1)}\right)$.*

3. *The numbers $\xi - a_1, \ldots, \xi - a_{n-1}$, form a full rank system of independent units of the field K_a.*

   (These numbers are called *basic ABC-units*. The multiplicative group, generated by the basic ABC-units, is called *the group of ABC-units*.)

4. *Assume that the field K_a is primitive*[1]*, and that the absolute value of its discriminant exceeds $|a|^\kappa$, where κ is a positive number. Then the group of ABC-units is of index at most $O\left(\kappa^{1-n}\right)$ in the group of all units.*

Proof Parts 1 and 2 are obvious. To prove Part 3, consider the real embeddings

$$\begin{aligned} \sigma_i : K_a &\to \mathbb{R} \\ \xi &\mapsto \xi_i \end{aligned} \qquad (i = 1, \dots, n-1). \tag{7}$$

Then (5) implies that $\log|\sigma_i(\xi - a_j)| = -\delta_{ij}\log|a| + O(1)$, where δ_{ij} is the Kronecker symbol. Hence,

$$R_{ABC} := \left|\det\left[\log|\sigma_i(\xi - a_j)|\right]_{1\le i,j\le n-1}\right| = (\log|a|)^{n-1} + O\left((\log|a|)^{n-3}\right).$$

In particular, $R_{ABC} \neq 0$ for sufficiently large $|a|$, which proves Part 3.

For Part 4, recall (cf. [24, 11]) that the regulator R and the discriminant D of a primitive field K satisfy the inequality $R \gg (\log|D|)^r$, where r is the rank of the unit group of K and the implicit constant depends on the degree of K. For the totally real field K_a we have $r = n-1$, which, together with the assumption $|D| \ge |a|^\kappa$, imply $R \gg (\kappa\log|a|)^{n-1}$. Hence, $R_{ABC}/R \ll \kappa^{1-n}$, as wanted. ■

(It might be pointed out that for sufficiently large $|a|$ the implicit constant in Part 4 depends only on n. For instance, using Theorem C of Friedman [11], one can show that for sufficiently large $|a|$ the index of the ABC-units in the group of all units does not exceed $Cn^{2n}\kappa^{1-n}$, where C is an absolute constant. We shall not use this more precise estimate.)

Sprindzhuk [26, Lemma 8.6.4] showed that, for $n \ge 3$, distinct ABC-fields are seldom isomorphic. Below, we reproduce his result in a slightly refined form.

Proposition 4.2 *(Sprindzhuk) Assume that $n \ge 3$. Let A be a sufficiently large positive integer, and let S be a set of integers a satisfying $A \le |a| \le 2A$ and such that for all $a \in S$ the fields K_a are isomorphic to the same field K. Then $|S| \le n(n-1)(n-2)$.*

Proof Assume that $|S| > n(n-1)(n-2)$. Since $\mathbb{R}$ has exactly n distinct subfields isomorphic to K, the set S has more than $(n-1)(n-2)$ elements a such that all the fields K_a are the same. Further, let $\sigma_i\colon K_a \to \mathbb{R}$ be defined as in (7). Then, for a given K_a, there exist $(n-1)(n-2)$ possibilities for the pair (σ_1, σ_2). Hence, there are distinct a and a' such that $K_a = K_{a'}$, $\sigma_1 = \sigma_1'$ and $\sigma_2 = \sigma_2'$. (Here and below $\xi', \xi_1', \dots, \xi_{n-1}', \sigma_1', \dots, \sigma_{n-1}'$ have the same meaning for a' as $\xi, \xi_1, \dots, \xi_{n-1}, \sigma_1, \dots, \sigma_{n-1}$ for a.) It follows that $\xi - \xi'$ is a non-zero algebraic integer from the field K_a, and $\sigma_i(\xi - \xi') = \xi_i - \xi_i'$ for $i = 1, 2$. Using (5) and the assumption $A \le |a|, |a'| \le 2A$, we obtain $|\xi - \xi'| \ll A$, as well as $|\sigma_i(\xi - \xi')| \ll A^{-1}$ for $i = 1, 2$ and $|\sigma_i(\xi - \xi')| \ll 1$ for $i = 3, \dots, n-1$. Hence

$$1 \le |\mathcal{N}_{K_a}(\xi - \xi')| = |\xi - \xi'| \prod_{i=1}^{n-1} |\sigma_i(\xi - \xi')| \ll A^{-1},$$

which is a contradiction for sufficiently large values of A. ■

5 Construction of the main polynomial

Starting from section, we begin the proof of Theorem 1.1. Until the end of the paper, we fix positive integers n and ℓ. Unless the contrary is stated explicitly, **we shall always assume that** $n \ge 3$.

In this section, we construct, for the given n and ℓ, a special polynomial in two variables, which will be used in the subsequent sections to produce Ankeny-Brauer-Chowla fields having required properties.

[1] that is, it has no proper subfield distinct from $\mathbb{Q}$.

Theorem 5.1 *There exists pairwise distinct non-zero integers $a_1, \ldots, a_{n-1}$ such that the polynomial*

$$f(t,x) := (x-a_1)\cdots(x-a_{n-1})\left(x-(-1)^{n-1}\frac{t^\ell-1}{a_1\cdots a_{n-1}}\right)-1 \in \mathbb{Q}[t,x] \tag{8}$$

has a symmetric Galois group over the field $\mathbb{Q}(t)$, and the polynomial $f(0,x)$ is separable.

Our starting point is the following result of Halter-Koch *et al.* [12, Proposition 3.1]:

Proposition 5.2 *Let K be a field, $\gamma \in K^*$ and $t_1, \ldots, t_n$ (algebraically independent) indeterminates over K. Then the Galois group of the polynomial $(x-t_1)\cdots(x-t_n)-\gamma$ over $K(t_1,\ldots,t_n)$ is $\mathcal{S}_n$.* ■

Proposition 5.3 *Let F be a field and H a finite Galois extension of F with Galois group $\mathcal{S}_n$, where $n \geq 4$. Let α an element of $\bar{F}$ such that $\alpha^\ell \in F$. Then $\mathrm{Gal}(H(\alpha)/F(\alpha))$ is either $\mathcal{S}_n$ or the alternating group $\mathcal{A}_n$.*

Proof Let ζ be a primitive ℓ-th root of unity and put $F_1 := F(\alpha,\zeta)$ and $H_1 := H(\alpha,\zeta)$. Since

$$\mathrm{Gal}(H_1/F_1) \leq \mathrm{Gal}(H(\alpha)/F(\alpha)) \leq \mathrm{Gal}(H/F) = \mathcal{S}_n,$$

it suffices to show that $\mathrm{Gal}(H_1/F_1) \geq \mathcal{A}_n$.

Since both H_1 and F_1 are Galois extensions of F, the group $\mathrm{Gal}(H_1/F_1) = \mathrm{Gal}\,(H/(H\cap F_1))$ is an invariant subgroup of $\mathcal{S}_n = \mathrm{Gal}(H/F)$. And it cannot be trivial because $\mathrm{Gal}(F_1/F)$ is a meta-abelian group, while $\mathcal{S}_n$ for $n \geq 4$ is not. It follows that $\mathrm{Gal}(H_1/F_1) \geq \mathcal{A}_n$, as wanted. ■

Proposition 5.4 *Let K be a field, $\alpha, \gamma \in K^*$, $\beta \in K$ and $n \geq 4$. Then the Galois group of the polynomial*

$$(x-t_1)\cdots(x-t_{n-1})\left(x-\frac{\alpha t^\ell+\beta}{t_1\cdots t_{n-1}}\right)-\gamma \tag{9}$$

over $K(t_1,\ldots,t_{n-1},t)$ is $\mathcal{S}_n$.

Proof Put

$$t_n := \frac{\alpha t^\ell+\beta}{t_1\cdots t_{n-1}}.$$

Proposition 5.2 implies that the Galois group of polynomial (9) over $K(t_1,\ldots,t_n)$ is $\mathcal{S}_n$. Using Proposition 5.3, we conclude that the Galois group of (9) over $K(t_1,\ldots,t_{n-1},t)$ is $\mathcal{S}_n$ or $\mathcal{A}_n$.

It remains to show that the x-discriminant of (9) is not a square in $K(t_1,\ldots,t_{n-1},t)$. It suffices to verify that the x-discriminant $D(t)$ of the polynomial $g(t,x) = (x-1)^{n-1}(x-\alpha t^\ell-\beta)-\gamma$ (obtained from (9) by specializing $t_1 = \ldots = t_{n-1} = 1$) is not a square in $K(t)$.

Put $a(t) = \alpha t^\ell+\beta-1$, so that $g(t) = (x-1)^{n-1}(x-1-a(t))-\gamma$. Then

$$\frac{\partial g}{\partial x}(x,t) = n(x-1)^{n-2}\left(x-1-\frac{n-1}{n}a(t)\right),$$

whence

$$D(t) = n^n g(t,1)^{n-2} g\left(t,\frac{n-1}{n}a(t)+1\right) = (-1)^{n-1}\gamma^{n-2}\left((n-1)^{n-1}a(t)^n+n^n\gamma\right).$$

Thus, $\deg D(t) = n\ell$ and $D'(t) = \delta a(t)^{n-2}t^{\ell-1}$, where $\delta \in K^*$. Since $D(t)$ does not vanish at the roots of $a(t)$, the only possible multiple root of $D(t)$ is 0, and if it is, its multiplicity is ℓ. Hence, $D(t)$ is not a square of a polynomial, as wanted. ■

Proposition 5.5 *Let K be a field, $\beta \in K$ and $\gamma \in K^*$. Assume that*[2]

$$(n-1)^{n-1}(\beta-1)^n + n^n\gamma \neq 0 \tag{10}$$

Then the polynomial

$$(x-t_1)\cdots(x-t_{n-1})\left(x-\beta t_1^{-1}\cdots t_{n-1}^{-1}\right)-\gamma \tag{11}$$

is separable over $K(t_1,\ldots,t_{n-1})$.

Proof Again, it suffices to show that the polynomial $g(x)=(x-1)^{n-1}(x-\beta)-\gamma$ (obtained from (11) by specializing $t_1=\ldots=t_{n-1}=1$) is separable over K. We have

$$g'(x) = n(x-1)^{n-2}\left(x-\frac{(n-1)\beta+1}{n}\right).$$

Since $g(1)=-\gamma\neq 0$ and $g\left(\frac{(n-1)\beta+1}{n}\right)\neq 0$ by (10), the result follows. ■

Proof of Theorem 5.1 One immediately verifies that $f_3(t,x)=(x^2-1)(x+t^\ell-1)-1$ is an irreducible over $\mathbb{Q}(t)$ polynomial in x, and its x-discriminant is not a square in $\mathbb{Q}(t)$. Hence, its Galois groups over $\mathbb{Q}(t)$ is $\mathcal{S}_3$. Since $f_3(0,x)$ is separable, this proves the theorem for $n=3$.

Assume now that $n\geq 4$ and consider the polynomial

$$F(t_1,\ldots,t_{n-1},t,x)=(x-t_1)\cdots(x-t_{n-1})\left(x-(-1)^{n-1}\frac{t^\ell-1}{t_1\cdots t_{n-1}}\right)-1\in\mathbb{Q}(t_1,\ldots,t_{n-1})[t,x].$$

Propositions 5.4 and 5.5 imply that the Galois group of F over $\mathbb{Q}(t_1,\ldots,t_{n-1},t)$ is $\mathcal{S}_n$, and that $F(t_1,\ldots,t_{n-1},0,x)$ is separable over $\mathbb{Q}(t_1,\ldots,t_{n-1})$.

By Theorem 2.2, there exists a thin set $\Upsilon\subseteq\mathbb{Q}^{n-1}$ such that for any $(\tau_1,\ldots,\tau_{n-1})\in(\mathbb{Q}^*)^{n-1}\setminus\Upsilon$, the Galois group of the specialized polynomial $F(\tau_1,\ldots,\tau_{n-1},t,x)$ is $\mathcal{S}_n$, and the polynomial $F(\tau_1,\ldots,\tau_{n-1},0,x)$ is separable. Finally, Theorem 2.3 implies that there exist pairwise distinct non-zero integers $a_1,\ldots,a_{n-1}$ such that $(a_1,\ldots,a_{n-1})\notin\Upsilon$. This completes the proof of the theorem. ■

6 Suitable integers

Recall that we fix positive integers n and ℓ with $n\geq 3$. In addition, starting from this point, we fix, once and for all, pairwise distinct non-zero integers $a_1,\ldots,a_{n-1}$ (which exist by Theorem 5.1) such that the polynomial $f(t,x)$, defined in (8), has Galois group $\mathcal{S}_n$ over $\mathbb{Q}(t)$, and the polynomial $f(0,x)$ is separable. Unless the contrary is stated explicitly, the constants in this section depend on n, ℓ and our particular choice of $a_1,\ldots,a_{n-1}$. In particular, *sufficiently large* means *of absolute value exceeding a positive constant depending on n, ℓ and the choice of $a_1,\ldots,a_{n-1}$.*

One immediately verifies that $f(0,0)=0$. Since $f(0,x)$ is a separable polynomial, it has a simple root at 0. Hence, $\frac{\partial f}{\partial x}(0,0)\neq 0$, and $a_1\cdots a_{n-1}\frac{\partial f}{\partial x}(0,0)$ is a non-zero integer.

Put

$$a(t):=(-1)^{n-1}\frac{t^\ell-1}{a_1\cdots a_{n-1}}.$$

Then $f(t,x)=(x-a_1)\cdots(x-a_{n-1})(x-a(t))-1$. If $\tau\in\mathbb{Z}$ satisfies

$$\tau\equiv 1 \mod a_1\cdots a_{n-1}, \tag{12}$$

then $a(\tau)\in\mathbb{Z}$ and $f(\tau,x)\in\mathbb{Z}[x]$. Moreover, for sufficiently large τ, this polynomial gives rise to the ABC-field $K_{a(\tau)}$, as defined in Proposition 4.1.

If the polynomial $f(\tau,x)$ has symmetric Galois group over $\mathbb{Q}$, then the field $K_{a(\tau)}$ is primitive. Hence, the following statement is a direct consequence of Proposition 4.1:4.

[2]This assumption can be dropped, but the argument would become slightly more involved.

Proposition 6.1 *There exists a positive integer N (depending on n, ℓ and the choice of $a_1, \dots, a_{n-1}$) with the following property. If the polynomial $f(\tau, x)$ has symmetric Galois group over $\mathbb{Q}$, and the discriminant of the field $K_{a(\tau)}$ exceeds $|\tau|^{2/(n+2)}$, then the index of the group of ABC-units in the group of all units does not exceed N.* ■

Definition 6.2 An integer τ is called *suitable* if it satisfies the following conditions.

1. We have (12) and $\gcd\left(\tau, a_1 \cdots a_{n-1} \frac{\partial f}{\partial x}(0,0)\right) = 1$.
2. The Galois group of the polynomial $f(\tau, x)$ (over $\mathbb{Q}$) is symmetric.
3. The discriminant of $K_{a(\tau)}$ exceeds $|\tau|^{2/(n+2)}$.
4. Let ξ be the root of $f(t,x) = (x-a_1)\cdots(x-a_{n-1})(x-a(\tau)) - 1$, as defined in Proposition 4.1:1. Then, for all integers $\nu, \nu_1, \dots, \nu_{n-1}$, satisfying
$$1 \le \nu \le N, \quad 0 \le \nu_1, \dots, \nu_{n-1} < \nu\ell, \tag{13}$$
where N is defined in Proposition 6.1, and for every determination of
$$\zeta = \left(\xi (\xi - a_1)^{\nu_1/\nu} \cdots (\xi - a_{n-1})^{\nu_{n-1}/\nu}\right)^{1/\ell},$$
we have $[K(\zeta)\colon K] \ge \ell$.

Theorem 6.3 *Put $\mu = \frac{1}{2\ell(n-1)}$. There exists a positive constant c (depending on n, ℓ and the choice of $a_1, \dots, a_{n-1}$) with the following property: for a large positive real number X there exist at least cX^μ suitable integers τ which give rise to pairwise non-isomorphic fields $K_{a(\tau)}$ of discriminants not exceeding X.*

Proof By Proposition 4.1:2, there exists a constant c_1 with the following property: for any $\tau \in \mathbb{Z}$, satisfying $|\tau| \le c_1 X^\mu$, the discriminant of the field $K_{a(\tau)}$ does not exceed X. Put $T := c_1 X^\mu$. Then at least $c_2 T$ integers τ satisfy
$$\left(\frac{T^\ell + 2}{2}\right)^{1/\ell} \le |\tau| \le T \tag{14}$$
and condition 1 of Definition 6.2.

Integers τ not satisfying conditions 2 and 4 of Definition 6.2 form a thin set (see Theorem 2.2 and Proposition 3.2). By Theorem 2.3, the number of such τ with $|\tau| \le T$ is $O\left(\sqrt{T}\log T\right)$. Inequality (2) implies that at most $O\left(\sqrt{T}\right)$ integers τ with $|\tau| \le T$ do not satisfy condition 3. It follows that at least $c_3 T$ suitable integers τ satisfy (14).

Finally, (14) implies that $A \le |a(\tau)| \le 2A$, where
$$A = \frac{T^\ell + 1}{2\,|a_1 \cdots a_{n-1}|}.$$
By Proposition 4.2, each $K_{a(\tau)}$ may occur at most $n(n-1)(n-2)$ times. Hence the theorem is proved with $c = c_3/(n(n-1)(n-2))$. ■

7 The ABC-field corresponding to a suitable integer

We are ready to complete the proof of Theorem 1.1. In view of Theorem 6.3, it remains to prove the following.

Proposition 7.1 *Let τ be a suitable integer. Then the class group of the field $K_{a(\tau)}$ has an element of exact order ℓ.*

Proof Since the suitable integer τ is fixed, we may omit the index and write $K = K_{a(\tau)}$. Since $f(0,0) = 0$, the polynomial $f(0,x)$ is divisible by x. Put $g(x) = a_1 \cdots a_{n-1} f(0,x)/x$. Then $g(x) \in \mathbb{Z}[x]$ and $g(0) = a_1 \cdots a_{n-1} \frac{\partial f}{\partial x}(0,0)$. In particular, $g(0) \neq 0$ and

$$\gcd(g(0), \tau) = 1. \tag{15}$$

Rewrite the equality $f(\tau, \xi) = 0$ as

$$\xi g(\xi) = (-1)^{n-1} (\xi - a_1) \cdots (\xi - a_{n-1}) \tau^{\ell}.$$

Since $\xi - a_1, \ldots, \xi - a_{n-1}$ are units, this implies the following equality for principal ideals: $(\xi)(g(\xi)) = (\tau)^{\ell}$. Relation (15) implies that ξ and $g(\xi)$ are coprime. Hence, each of the principal ideals (ξ) and $(g(\xi))$ is an ℓ-th power of an ideal of K.

Let $\mathfrak{a}$ be the ideal of K such that $\mathfrak{a}^{\ell} = (\xi)$. The order λ of the class of $\mathfrak{a}$ in the class group divides ℓ, and **we wish to prove that $\lambda = \ell$.**

The ideal $\mathfrak{a}^{\lambda}$ is principal. Fix $\alpha \in K$ such that $\mathfrak{a}^{\lambda} = (\alpha)$ and let ζ be some determination of $\alpha^{1/\lambda}$. Then

$$[K(\zeta) \colon K] \leq \lambda \leq \ell. \tag{16}$$

Let ν be the index of ABC-units in the group of all Dirichlet units of the field K. Then any unit of K can be presented as (a suitable determination of) $(\xi - a_1)^{\nu_1/\nu} \cdots (\xi - a_{n-1})^{\nu_{n-1}/\nu}$, where $\nu_1, \ldots, \nu_{n-1} \in \mathbb{Z}$. In particular, since $\zeta^{\ell} \in K$ and $\left(\zeta^{\ell}\right) = (\xi)$, we have

$$\zeta^{\ell} = \xi \, (\xi - a_1)^{\nu_1/\nu} \cdots (\xi - a_{n-1})^{\nu_{n-1}/\nu}. \tag{17}$$

Multiplying ζ by a suitable ABC-unit, we may assume that the integers $\nu_1, \ldots, \nu_{n-1}$ in (17) satisfy $0 \leq \nu_1, \ldots, \nu_{n-1} < \nu\ell$. Also, since the Galois group of the polynomial $f(\tau, x)$ is symmetric, Proposition 6.1 implies that $\nu \leq N$.

Thus, ζ satisfies (17), where the integers $\nu, \nu_1, \ldots, \nu_{n-1}$ satisfy (13). Hence, $[K(\zeta) \colon K] \geq \ell$. Together with (16), this implies $\lambda = \ell$, as wanted. This completes the proof of Proposition 7.1 and of Theorem 1.1. ■

8 Final remarks

1. Though we do not specifically consider the effectivity aspect in this note, one may check that our argument effectively bounds the constants X_0 and c from Theorem 1.1 in terms of ℓ and n.
2. The estimate $\left|\mathcal{F}_n^{(\ell)}\right| \gg X^{\mu}$ can be, probably, slightly refined by letting the parameters $a_1, \ldots, a_{n-1}$ vary.
3. Theorem 1.1 can be refined to count number fields with a given number of real and complex embeddings. For this purpose, one should simply replace our totally real ABC-fields by fields with r real and $2s$ complex embeddings, defined by polynomials of the type

   $$(x - a_1) \cdots (x - a_r) \left(x^2 + b_1 x + c_1\right) \cdots \left(x^2 + b_s x + c_s\right) \pm 1$$

   with $b_j^2 - 4c_j < 0$.

Some of these points will be addressed in the forthcoming Ph.D. thesis of S. Hernández.

References

[1] N.C. Ankeny, R. Brauer, S. Chowla, A note on the class-numbers of algebraic number fields, *Amer. J. Math.* **78** (1956), 51–61.

[2] N.C. Ankeny, S. Chowla, On the divisibility of the class number of quadratic fields, *Pacific J. Math.* **5** (1955), 321–324.

[3] T. Azuhata, H. Ichimura, On the divisibility problem of the class numbers of algebraic number fields, *J. Fac. Sci. Univ. Tokyo* **30** (1984), 579–585.

[4] Z.I. Borevich, I.R. Shafarevich, *Number theory*, Academic Press, London-New York, 1966.

[5] K. Chakraborty, M.R. Murty, On the number of real quadratic fields with class number divisible by 3, *Proc. Amer. Math. Soc.* **131** (2003), 41–44.

[6] H. Cohen, *Advanced Topics in Computional Number Theory*, Graduate Texts in Mathematics **193**, Springer, 2000.

[7] H. Cohen, H.L. Lenstra, Jr., Heuristics on class groups of number fields, *Springer Lecture Notes in Math.* **1068** (1984), 33–62.

[8] H. Cohen, J. Martinet, Étude heuristique des groupes de classes des corps de nombres, *J. r. angew. Math.* **404** (1990), 39–76.

[9] S.D. Cohen, The distribution of Galois groups and Hilbert irreducibility theorem, *Proc London Math. Soc.* **43** (1981), 227–250.

[10] J.S. Ellenberg, A. Venkatesh The number of extensions of a number field with fixed degree and bounded discriminant, submitted.

[11] E. Friedman, Analytic formulas for the regulator of a number field, *Invent. Math.*, **98** (1989), 599–622.

[12] F. Halter-Koch, G. Lettl, A. Pethő, R.F. Tichy, Thue equations associated with Ankeny-Brauer-Chowla number fields, *J. London Math. Soc.* **60** (1999), 1–20.

[13] S. Hernández, F. Luca, Divisibility of exponents of class groups of cubic number fields, preprint, 2003.

[14] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[15] F. Luca, A note on the divisibility of class numbers of real quadratic fields, *C. R. Math. Acad. Sci. Soc. R. Can.*, to appear.

[16] M.R. Murty, Exponents of class groups of quadratic number fields, *Topics in Number Theory (University Park, PA; 1997)* Kluwer Acad. Publ., Dordrecht, 1999, 229–239.

[17] T. Nagell, Über die KlassenZahl imaginär-quadratischer Zahlkörper, *Abh. math. Sem. Univ. Hamburg* **1** (1922), 140–150; see also: *Collected papers of Trygve Nagell* (ed. P. Ribenboim), Queens University Press, Kingston, 2002, vol. 1, pp. 197–209.

[18] S. Nakano, On the construction of certain number fields, *Tokyo J. Math.* **6** (1983), 389–395.

[19] S. Nakano, On ideal class groups of algebraic number fields, *J. Reine Angew. Math.* **358** (1985), 61–75.

[20] S. Nakano, Ideal class groups of cubic cyclic fields, *Acta Arith. 46* (1986), 297-300.

[21] G. Pólya, G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Zweiter Band, Dritte Auflage, Springer, 1964.

[22] W.M. Schmidt, Number fields of given degree and bounded discriminant, *Astérisque* **228** (1995), 189-195.

[23] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, 3rd edition, Aspects in Mathematics **E 15**, Vieweg, 1997.

[24] J.H. Silverman, An inequality relating the regulator and the discriminant of a number field, *J. Number Theory* **19** (1984), 437-442.

[25] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc. (2)* **61** (2000), 681–690.

[26] V.G. Sprindzhuk, *Classical Diophantine Equations in Two Unknowns* (Russian), Nauka, Moscow, 1982; English trans.: Lecture Notes in Math., Vol. 1559, Springer, 1994.

[27] K. Uchida, Class numbers of cubic cyclic fields, *J. Math. Soc. Japan* **26** (1974), 447–453.

[28] P.J. Weinberger, Real quadratic fields with class nuumbers divisible by n, *J. Number Theory* **5** (1973), 237–241.

[29] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), 57–76.

[30] G. Yu, A note on the divisibility of class numbers of real quadratic fields, *J. Number Theory* **97** (2002), 35–44.

Yuri F. Bilu
A2X
Université de Bordeaux 1
351 Cours de la Libération
33405 Talence
FRANCE
yuri@math.u-bordeaux.fr

Florian Luca
Mathematical Institute
UNAM
Ap. Postal 61-3 (Xangari)
CP 58 089, Morelia, Michoacán
MEXICO
fluca@matmor.unam.mx